

Paper Reference 20158K
Pearson BTEC
Level 3 Nationals Diploma,
Extended Diploma,

Total Marks

INFORMATION TECHNOLOGY
UNIT 11: CYBER SECURITY AND
INCIDENT MANAGEMENT

(PART B)

Window for supervised period:

Monday 7 January 2019 – Friday 25 January 2019

**Supervised hours: 4 hours (plus your additional
time allowance)**

**In the boxes below, write your name, centre number
and candidate number.**

Surname					
Other names					
Centre Number					
Candidate Number					

X61675A

ITEMS INCLUDED WITH QUESTION PAPER

- **A Separate Diagram Booklet.**
- **Instructions to Teachers/Tutors and/or Invigilators.**
- **Instructions for Learners.**
- **Set Task Brief.**

YOU MUST HAVE:

- **Forensic_Analysis.rtf**

INSTRUCTIONS

- **Part A and Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set task of 80.
- **Part A and Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 4 – hour, **Part B** supervised assessment period.

- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3 – week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- **Part A** materials must not be accessed during the completion of **Part B**.
- This booklet should not be returned to Pearson.
- Answer ALL activities.

INFORMATION

- The total mark for this paper is 37.
-

PART B SET TASK

YOU MUST COMPLETE ALL ACTIVITIES IN THE SET TASK.

PRODUCE YOUR DOCUMENTS USING A COMPUTER.

SAVE YOUR DOCUMENTS IN YOUR FOLDER READY FOR SUBMISSION USING THE FORMATS AND NAMING CONVENTIONS INDICATED.

READ THE SET TASK BRIEF CAREFULLY BEFORE YOU BEGIN AND NOTE THAT READING TIME IS INCLUDED IN THE OVERALL ASSESSMENT TIME.

You advised Peter and Elana on security matters. Now, a few months later, Elana has called you in to review the investigation of a cyber security incident.

Activity 4 is on the next page.

ACTIVITY 4: FORENSIC INCIDENT ANALYSIS

Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident at Romwebhost.

Consider possible causes of the incident and come to a conclusion about the most likely cause of the incident.

Refer to evidence items 1 – 4 inclusive in the Set Task Brief.

Produce a forensic incident analysis using the template **Forensic_Analysis.rtf**

Save your completed forensic incident analysis as a PDF in your folder for submission as **activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity (plus your additional time allowance).

(TOTAL FOR ACTIVITY 4 = 14 MARKS)

Activity 5 is on the next page.

Turn over

ACTIVITY 5: SECURITY REPORT

Review the incident. Suggest improvements and explain how they would prevent a similar incident in the future.

Areas for improvement are:

- **adherence to forensic procedures**
- **the forensic procedure and current security protection measures**
- **the security documentation.**

Read the Set Task Brief and evidence items 1 – 5 inclusive when answering the question.

**Save your completed security report as a PDF in your folder for submission as
activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity (plus your additional time allowance).

(TOTAL FOR ACTIVITY 5 = 20 MARKS)

**TOTAL FOR TECHNICAL LANGUAGE IN
TASK B = 3 MARKS**

TOTAL FOR PAPER = 37 MARKS
